CvB stukken voor agenda Universiteitsraad

Overlegvergadering d.d. : 24-4-2019
Commissievergadering : --
Agendapunt : Digital codes of conduct
(students, employees, ICT-employees)
Bijgevoegde stukken :

- Digitale gedragscode - studenten - v1.9
- Digitale gedragscode - medewerkers - v2.0
- Gedragscode ICT-functionarissen - v1.7

Betrokken dienst: LISA paraaf: JC

Secretaris: Wichman paraaf:

Portefeuillehouder: Bult paraaf:

---

1. **Status agendapunt:**
   Rol URaad:
   - o Ter informatie
   - o Ter advisering
   - ✓ Ter instemming
   - o Anders:

---

2. **Eerder behandeld in:**
   Naam gremium: UCB
   Datum behandeling: 26-02-2019
   Naam agendapunt: actualisering digitale gedragscodes medewerkers, studenten, ICT-functionarissen
   Conclusie toen: positive advice

---

3. **Toelichting/samenvatting (engelstalig):**

With the digital codes of conduct for students and employees the university sets rules for how to use the ICT facilities of the university in a safe and responsible way. The code of conduct for ICT-employees sets additional rules for employees who perform tasks within the ICT-domain.

The current versions of these codes of conduct are from the period 2009-2012.
The documents have now been updated. Main changes concern:
- Connection with SURF's current templates documents (not for the code of conduct for ICT employees, because of the very legal language)
- Actualization regarding legislation (especially GDPR – General Data Protection Regulation, AVG in Dutch) and current state of technology
- Deduplication with other policy documents established in the intervening period

The documents were reviewed in the security and privacy workgroup and legally checked by HR, including being WNRA-proof.

4. <u>(Voorgenomen) besluit CvB</u>:

Gezien
Gehoord
Overwegende
Besluit het CvB:

The Executive Board decides to establish the digital code of conduct for students, version 1.9, the digital code of conduct for employees, version 2.0 and the code of conduct ICT-employees, version 1.7.

GRIFFIE URaad: (door griffie UR in te vullen)
<u>Eerder in URaad aan de orde geweest?</u>

- ✓ Nee.
- o Ja, op
  Conclusie toen:

<u>Nadere toelichting:</u> (Voor als presidium/griffier vindt dat één van bovengenoemde punten nadere toelichting behoeft)

.....
.....

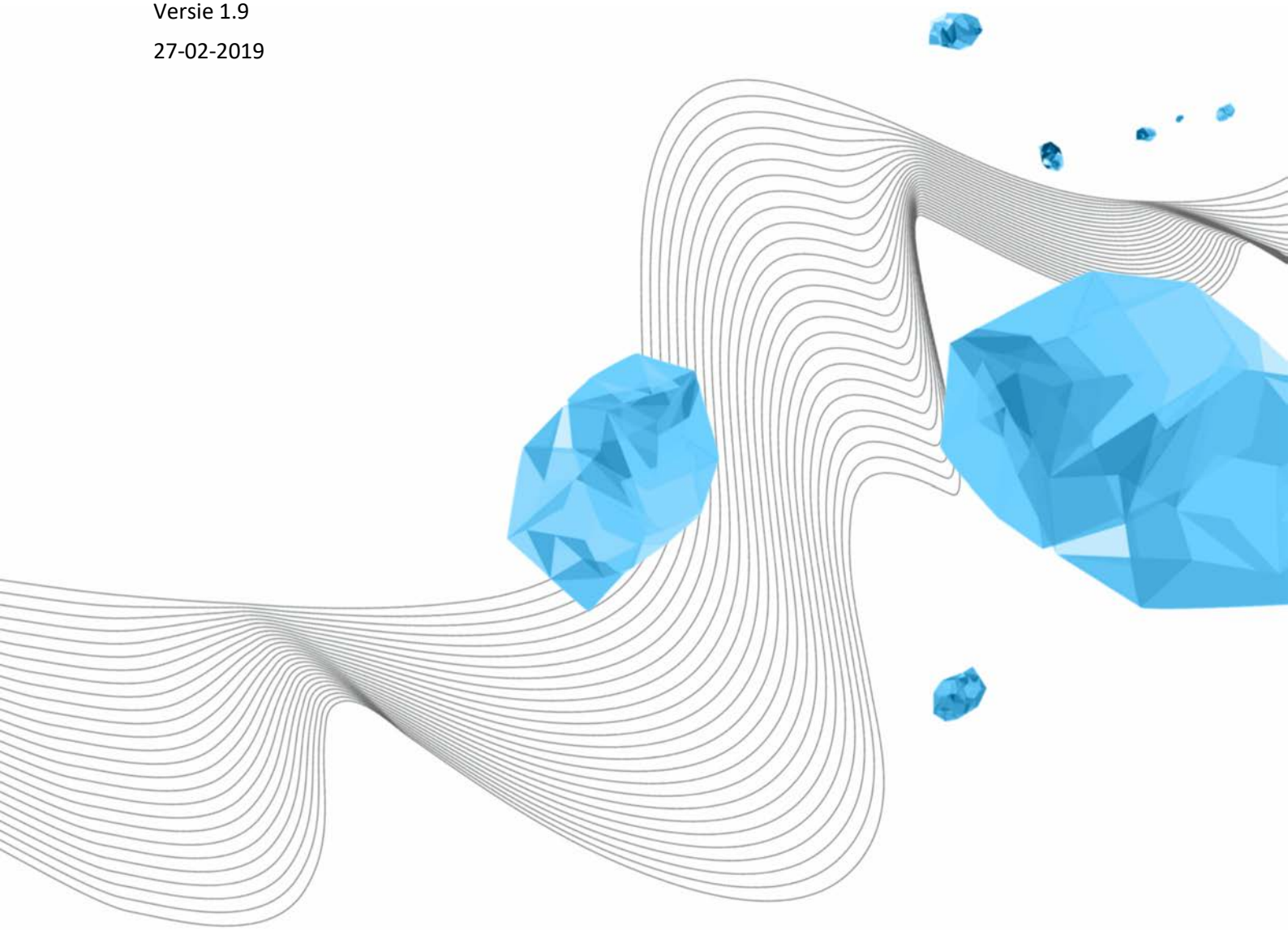
C O N C E P T

DIGITALE GEDRAGSCODE VOOR STUDENTEN UNIVERSITEIT TWENTE

Brake - Loeve, A.A. te (LISA)

Versie 1.9

27-02-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Digitale gedragscode voor studenten Universiteit Twente

KENMERK
UIM/181205/brk

VERSIE (STATUS)
1.9

DATUM
27-02-2019

AUTEUR(S)
Brake - Loeve, A.A. te (LISA)

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	2011	Wim Koolhoven	Definitieve versie
1.4	19-11-2018	Rianne te Brake	Herziene versie: - Structuur volgens actuele SURF model - Actualisatie voor wat betreft stand techniek, privacywetgeving (AVG) - Onderdelen geschrapt die intussen in zelfstandige documenten zijn opgenomen
1.6	20-12-2018	Rianne te Brake	Reacties verwerkt, wijziging sjabloon
1.7	15-01-2019	Jan Evers	Opmerkingen MT LISA verwerkt
1.8	06-02-2019	Jan Evers	Opmerkingen MT LISA en Harma Evers verwerkt
1.9	26-02-2019	Jan Evers	Positief advies UCB

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.4	22-11-2018	Rianne te Brake	Jan Evers, Henk Swaters, Marc Berenschot, Peter Peters, Erna van der Zandt, Wim Olijslager (security & privacy overleg)
1.6	20-12-2018	Jan Evers	MT LISA
1.7	15-01-2019	Jan Evers	MT LISA, HR – Harma Evers
1.8	06-02-2019	Jan Evers	UCB
1.9	27-02-2019	Jan Evers	CvB

REFERENTIES

VERSIE	DATUM	AUTEUR(S)	TITEL

INHOUDSOPGAVE

1 BRONVERMELDING

De Digitale gedragscode voor studenten van de Universiteit Twente is gebaseerd op het Model Acceptable Use Policy voor studenten voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo. Deze publicatie is beschikbaar onder de licentie Creative Commons Naamsvermelding 3.0 Nederland[1].

2 INLEIDING

De Universiteit Twente (hierna: “de Universiteit”) biedt aan de eigen studenten en aan bezoekende studenten de mogelijkheid internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik ten behoeve van de studie een mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld. Aan het gebruik van deze faciliteiten zijn regels verbonden. Tegen deze achtergrond mag van studenten verantwoord gebruik van internet en ICT worden verwacht.
Deze gedragscode geldt voor elke student die is ingeschreven bij de Universiteit, onderwijs volgt bij de Universiteit of een studentencampuswoning bewoont en die gebruik maakt van de door de Universiteit geboden ICT-faciliteiten. Daarnaast is deze regeling van toepassing op ex-studenten die vallen onder de Regeling ICT-faciliteiten ex-UT-ers.

3 GEBRUIK VAN FACILITEITEN

Computer- en netwerkfaciliteiten (zoals openbare computers, (software-)licenties, draadloze en vaste netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgeving) worden aan de student beschikbaar gesteld ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten. Wanneer de Universiteit voor onderwijsdoeleinden specifieke systemen voorschrijft, zal de student alleen deze systemen gebruiken voor de betreffende doeleinden en de daarbij gestelde beperkingen en eisen stipt naleven.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de Universiteit is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement en de licentievoorwaarden van de leverancier. Het aanbrengen van veranderingen in apparatuur en toepassingen beschikbaar gesteld door de Universiteit is alleen toegestaan met aparte toestemming van systeembeheer. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de vaste of draadloze netwerkaansluitingen is te allen tijde verboden, behalve in de woonruimte van studenten.

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord en/of authenticatiemiddel zoals een applicatie op een smartphone. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. Het systeembeheer kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een vermoeden van misbruik van een wachtwoord of authenticatiemiddel kan per direct het betreffende account ontoegankelijk worden gemaakt.

[1] www.creativecommons.org/licenses/by/3.0/nl.

4 INTELLECTUEEL EIGENDOM EN VERTROUWELIJKE INFORMATIE

De student maakt geen inbreuk op de intellectuele eigendomsrechten van de Universiteit en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Universiteit.

Indien de student in het kader van zijn studie of het uitvoeren van taken voor de Universiteit toegang krijgt tot vertrouwelijke informatie of privacygevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen.
De student besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke informatie buiten de Universiteit noodzakelijk is, zoals via e-mail, in niet Universiteitsgebonden cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, tablets, etc.).

Indien de Universiteit met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld dient de student deze stipt op te volgen.

5 BEVEILIGING DOOR DE UNIVERSITEIT ÉN DE STUDENT

De Universiteit neemt informatiebeveiliging serieus. Zij hanteert dan ook een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten. Perfecte beveiliging is onmogelijk. Daarom verwacht de Universiteit ook van studenten een proactieve houding om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. De student is te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens. De student treft beveiligingsmaatregelen conform de adviezen en aanwijzingen van het cybersafety-team van de Universiteit[2].

6 PRIVÉGEBRUIK EN OVERLAST

Beperkt privégebruik van de ICT- en internetfaciliteiten is toegestaan. Gebruik, privé of ten behoeve van studie, mag niet storend zijn voor de goede orde bij de Universiteit en mag geen overlast veroorzaken bij anderen, mag geen inbreuk maken op rechten van de Universiteit of derden of de integriteit en de veiligheid van het netwerk aantasten. Daarnaast geldt dat privégebruik alleen is toegestaan wanneer de licentievoorwaarden van de leverancier dit toelaten. De Universiteit is niet verplicht reservekopieën te maken van opgeslagen privébestanden of –informatie op systemen van de Universiteit of hiermee rekening te houden bij vervanging of reparatie van betreffende systemen. Als verboden, storend en/of overlast veroorzakend gebruik geldt:

[2] Bijvoorbeeld het Cybersafety 10-stappenplan.

- het in openbare ruimtes raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware.

Studenten die in hun privé woonruimte met privé middelen gebruik maken van een netwerkfaciliteit van de Universiteit kunnen geen beperkingen opgelegd worden aan het gebruik, behoudens voor zover noodzakelijk om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om de gevolgen van overbelasting te beperken. Indien de Universiteit ingrijpt om de gevolgen van overbelasting te beperken, zullen gelijke soorten verkeer gelijk worden behandeld. De overige bepalingen in dit reglement zijn onverkort van toepassing voor studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Universiteit.
Het gebruik van computer- en netwerkfaciliteiten ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer de Universiteit hiervoor schriftelijk toestemming heeft verleend.

7 MONITORING DOOR DE UNIVERSITEIT

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit deze gedragscode ten behoeve van de goede orde op de Universiteit en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van de Universiteit.
Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor verwerkingsverantwoordelijke of medewerkers met een toezichthoudende taak in het kader van een gericht onderzoek. Deze gegevens worden alleen in geanonimiseerde vorm aan overige medewerkers beschikbaar gesteld, tenzij dit onmogelijk is voor het uitvoeren van beheertaken.
In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet men zo snel mogelijk daarna melding van de maatregel.
Bij vermoedens van overtreding van de regels uit deze gedragscode kan het CvB opdracht geven tot het uitvoeren van een gericht onderzoek (zie paragraaf 8).
De Universiteit houdt zich bij het uitvoeren van een gericht onderzoek onverkort aan de Algemene Verordening Gegevensbescherming en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Universiteit de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang.
E-mailberichten van Universiteitsraadleden, faculteitsraadleden en leden van de opleidingscommissies in functie worden niet gecontroleerd voor zover deze betrekking hebben op hun functie als lid van de medezeggenschap/opleidingscommissie. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

8 GERICHT ONDERZOEK

Bij zwaarwegende vermoedens van overtreding van deze, of andere, gedragscode door een medewerker heeft de UT het recht om een gericht onderzoek uit te voeren. Voor het uitvoeren van een gericht onderzoek is altijd een opdracht vanuit het CvB nodig. De UT garandeert dat een gericht onderzoek op een zorgvuldige manier wordt uitgevoerd.

9 CONSEQUENTIES VAN OVERTREDING

Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het College van Bestuur van de Universiteit afhankelijk van de aard en de ernst van de overtreding maatregelen treffen.
Hieronder vallen een waarschuwing, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.
Maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Hiervoor is altijd menselijke beoordeling nodig. Voorts worden geen maatregelen getroffen zonder dat de student gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.
In afwijking van het voorgaande is het mogelijk dat de Universiteit bij (geautomatiseerde) constatering van overlast of een beveiligingsrisico een tijdelijke blokkade van de betreffende faciliteit invoert.
Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van het systeembeheer is weggenomen. Indien na een week geen verbetering is geconstateerd door het systeembeheer, kan het systeembeheer besluiten tot een langere blokkade.
Bij herhaling van de oorzaak kunnen maatregelen worden genomen.

10 SLOTBEPALINGEN

Deze gedragscode wordt tweejaarlijks geëvalueerd. Wijzigingen worden alleen ingevoerd nadat de Universiteitsraad heeft ingestemd. Het College van Bestuur kan feedback van studenten in overweging nemen alvorens de wijzigingen in te voeren.
In gevallen waarin deze gedragscode niet voorziet, beslist het College van Bestuur.
Deze gedragscode vervangt de Gedragscode ICT- en internetgebruik Universiteit Twente studenten 2011.

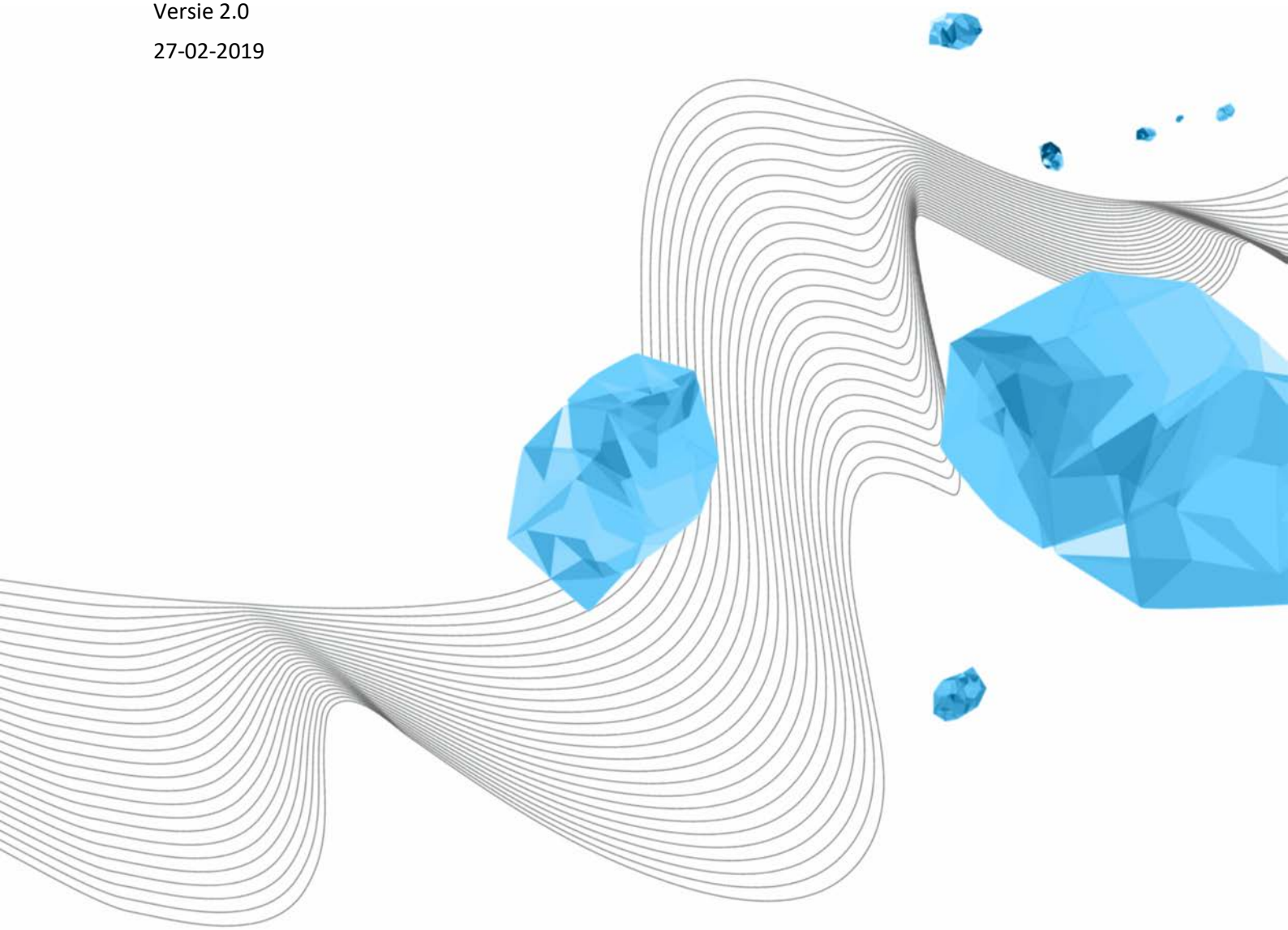
C O N C E P T

DIGITALE GEDRAGSCODE VOOR MEDEWERKERS UNIVERSITEIT TWENTE

Brake - Loeve, A.A. te (LISA)

Versie 2.0

27-02-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Digitale gedragscode voor medewerkers Universiteit Twente

KENMERK
UIM/181204/brk

VERSIE (STATUS)
2.0

DATUM
27-02-2019

AUTEUR(S)
Brake - Loeve, A.A. te (LISA)

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	2009	Wim Koolhoven	Definitieve versie
1.1	15-06-2018	Rianne te Brake	Herziene versie: - Structuur volgens actuele SURF model - Actualisatie voor wat betreft privacywetgeving (AVG) en stand techniek - Onderdelen geschrapt die in zelfstandige documenten zijn opgenomen
1.6	04-12-2018	Rianne te Brake	Sjabloon aangepast, reacties verwerkt
1.8	15-01-2019	Jan Evers	Opmerkingen MT LISA verwerkt
1.9	06-02-2019	Jan Evers	Opmerkingen MT LISA en Harma Evers verwerkt (o.a. WNRA-check)
2.0	26-02-2019	Jan Evers	Positief advies UCB

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.1	15-06-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager (security & privacy overleg)
1.6	06-12-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager
1.8	15-01-2019	Jan Evers	MT LISA, HR – Harma Evers
1.9	06-02-2019	Jan Evers	UCB
2.0	27-02-2019	Jan Evers	CvB

REFERENTIES

VERSIE	DATUM	AUTEUR(S)	TITEL

INHOUDSOPGAVE

1 BRONVERMELDING

De Digitale gedragscode voor medewerkers van Universiteit Twente, verder aangeduid als de Universiteit, is gebaseerd op het Model Acceptable Use Policy voor medewerkers voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo. Deze publicatie is beschikbaar onder de licentie Creative Commons Naamsvermelding 3.0 Nederland[1].

2 BASIS VOOR DE GEDRAGSCODE

Het gebruik van het interne computernetwerk en het openbare computernetwerk (internet) en ICT-middelen die door de Universiteit beschikbaar worden gesteld, is voor (veel van) de medewerkers van de Universiteit noodzakelijk om hun werk goed te kunnen doen. Aan het gebruik van deze faciliteiten zijn risico's verbonden, om deze te verminderen zijn medewerkers gehouden aan gedragsregels van de Universiteit. Tegen de achtergrond hiervan mag van de medewerkers verantwoord gebruik van internet en ICT worden verwacht.

Met deze gedragscode stelt de Universiteit regels omtrent het gewenst gebruik van deze bedrijfsmiddelen. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van de medewerker.
Het gebruik van social media zoals Facebook, LinkedIn en Twitter wordt steeds belangrijker maar kan ook zijn weerslag hebben op de Universiteit. Daarom stelt de Universiteit ook hier bepaalde regels aan.
De Universiteit is als werkgever bevoegd regels te stellen omtrent de uitvoering van het werk en de goede orde op de werkvloer, zo volgt uit de wet.
Omdat de Gedragscode voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van medewerkers, is de Universiteitsraad instemmingsplichtig.

3 ARTIKELEN

3.1 ARTIKEL 1. UITGANGSPUNTEN

1.1. Beperkt privégebruik van internet en ICT-middelen is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of het netwerk van de Universiteit. De Universiteit is echter niet verplicht van privé-bestanden reservekopieën te maken of kopieën beschikbaar te stellen bij vervanging of reparatie van de betreffende systemen. Gebruik voor nevenwerkzaamheden is uitsluitend toegestaan als en voor zover de Universiteit hiervoor schriftelijk toestemming heeft verleend.
1.2. Deze gedragscode geldt voor iedereen die voor de Universiteit werkzaam is, dus ook voor uitzendkrachten en tijdelijke medewerkers. Daarnaast is deze gedragscode van toepassing op ex-medewerkers die vallen onder de Regeling ICT-faciliteiten ex-UT-ers. Voor gasten van medewerkers die gebruik maken van de ICT-voorzieningen van de Universiteit geldt deze gedragscode eveneens.
1.3. De gedragscode geldt niet voor (gast)studenten; hiervoor is een aparte gedragscode opgesteld. Deze code geldt wel onverkort voor studenten die tevens in dienst zijn bij de Universiteit.
1.4. De Universiteit streeft in het kader van handhaving van deze gedragscode naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel

[1] www.creativecommons.org/licenses/by/3.0/nl.

mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

1.5. Elke medewerker draagt zoveel mogelijk zelf verantwoordelijkheid voor het verantwoord en veilig gebruiken van de ICT- en internetvoorzieningen van de Universiteit.

3.2 ARTIKEL 2. VERTROUWELIJKE INFORMATIE

2.1 De medewerker dient vertrouwelijke informatie en privacygevoelige informatie waaronder persoonsgegevens, waar hij in het kader van het werk toegang toe heeft, strikt vertrouwelijk te behandelen en voldoende maatregelen te treffen om de vertrouwelijkheid te waarborgen.

2.2 De medewerker treft beveiligingsmaatregelen conform de adviezen en aanwijzingen van het cybersafety-team van de Universiteit[2].

3.3 ARTIKEL 3. GEBRUIK VAN ICT-VOORZIENINGEN

3.1 ICT-voorzieningen waaronder begrepen computer- en netwerkfaciliteiten, (software-)licenties, e-mail en andere ICT-communicatiemiddelen en internet, worden aan de medewerker voor gebruik in het kader van zijn functie beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit deze functie.

3.2 Privégebruik en gebruik voor nevenwerkzaamheden van deze middelen is alleen toegestaan zoals bepaald in artikel 1.1 en alleen als de licentievoorwaarden van de leverancier dit toestaan.

3.3 De medewerker dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens). Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld. Bij een vermoeden van misbruik van een wachtwoord kan het systeembeheer per direct het betrokken account ontoegankelijk maken.

3.4 De Universiteit kan voor onderwijs-, onderzoek- en andere bedrijfsdoeleinden systemen of applicaties voorschrijven, zoals een elektronische leeromgeving, een emailsysteem, (mobiele) applicaties (apps) of multimediadiensten. De medewerker zal voor de betreffende doeleinden alleen deze systemen gebruiken en de daarbij gestelde beperkingen en eisen stipt naleven.

3.5 Gebruik van de faciliteiten (privé of niet) mag niet storend zijn voor de goede orde op de Universiteit en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Universiteit of derden of de integriteit en de veiligheid van het netwerk aantasten.
Tenminste verboden bij elk gebruik (privé of niet) van ICT-voorzieningen is:

- het bezoeken van sites of verzenden van berichten met een pornografische, racistische, discriminerende, bedreigende, beledigende of aanstootgevende inhoud, tenzij dit noodzakelijk is voor de vrije informatievergaring in het kader van de functie-uitoefening en hiervoor toestemming is verkregen van de beheerder;
- het verzenden van berichten met een (seksueel) intimiderende inhoud;
- het verzenden van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van kettingbrieven, spam of kwaadaardige software zoals virussen, Trojaanse paarden of spyware
- het gebruik van filesharing- of streamingdiensten, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen.

3.6 De medewerker gebruikt voor privémail bij voorkeur een ander dan het door de Universiteit verstrekte e-mailadres, binnen de grenzen van artikel 1.1. De Universiteit zal de toegang tot andere e-maildiensten niet blokkeren of specifiek monitoren.

3.7 De medewerker verstrekt een privé e-mailadres aan de Universiteit, onder andere ten behoeve van het beheer van zijn account.

3.8 De medewerker is bij beëindiging van het dienstverband verplicht de apparatuur van de Universiteit in te leveren, inclusief de bijbehorende toegangscodes.

[2] Bijvoorbeeld het Cybersafety 10-stappenplan.

3.9 Het aansluiten van actieve netwerkcomponenten (zoals access-points en routers) is niet toegestaan zonder schriftelijke toestemming van LISA netwerkbeheer.

3.4 ARTIKEL 4. GEBRUIK VAN SOCIALE MEDIA

4.1 De Universiteit ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met vakgenoten en derden via sociale media. Indien dit werk gerelateerde onderwerpen betreft, dient de medewerker ervoor te zorgen dat het profiel en de inhoud in overeenstemming zijn met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en studenten.

4.2 Bestuurders, managers, leidinggevenden en anderen die namens de Universiteit beleid of strategie uitdragen of een representatieve functie vervullen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij afwegen of zij op persoonlijke titel kunnen publiceren.

4.3 Dit artikel geldt ook indien medewerkers vanaf privécomputers of -internetaansluitingen deelnemen aan sociale media, doch uitsluitend voor zover het gaat om deelname die het werk kan raken.

4.4 De medewerker draagt bij beëindiging van het dienstverband werkgerelateerde sociale-media-accounts over aan de Universiteit.

3.5 ARTIKEL 5. MONITORING EN CONTROLE

5.1 Controle van gebruik van de ICT-voorzieningen vindt slechts plaats in het kader van handhaving van de regels uit deze gedragscode.

5.2 Ten behoeve van controle op de naleving van de regels worden gegevens geautomatiseerd verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de verwerkingsverantwoordelijke of medewerkers met een toezichthoudende taak in het kader van een gericht onderzoek. Deze gegevens worden alleen in geanonimiseerde vorm aan overige medewerkers beschikbaar gesteld, tenzij dit onmogelijk is voor het uitvoeren van beheertaken.

5.3 Bij vermoedens van overtreding van de regels uit deze gedragscode kan het CvB opdracht geven tot het uitvoeren van een gericht onderzoek (zie paragraaf 3.6).

5.4 De Universiteit houdt zich bij het uitvoeren van een gericht onderzoek onverkort aan de Algemene Verordening Gegevensbescherming en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Universiteit de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang.

5.5 E-mailberichten van leden van een medezeggenschapsorgaan onderling, van bedrijfsartsen, van HR-functionarissen en van eenieder die zich op grond van de wet op vertrouwelijkheid mag beroepen, worden niet gecontroleerd. Dit geldt niet voor geautomatiseerde controle op de veiligheid van het e-mailverkeer en netwerk.

5.6 In geval van ziekte, onverwacht langdurige afwezigheid of grove nalatigheid van de medewerker, doch uitsluitend als dit een zwaarwegende reden van bedrijfsbelang tot toegang oplevert, is de Universiteit gerechtigd een vervanger / leidinggevende toegang tot de bestanden of mailbox van de medewerker te verschaffen. Dit is uitsluitend toegestaan indien aangetoond kan worden dat toestemming van de medewerker verkrijgen onmogelijk is of het bedrijfsbelang zodanig zwaar is dat toestemming niet gevraagd kan worden en na toestemming van het College van Bestuur. De vervanger / leidinggevende mag zich echter geen toegang verschaffen tot als privé gemarkeerde mappen, als privé herkenbare mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon, een bedrijfsarts of een HR-functionaris. Alvorens de vervanger of leidinggevende toegang krijgt, schakelt de Universiteit een medewerker van CERT-UT, een vertrouwenspersoon en / of een HR-adviseur in om de betreffende informatie van de medewerker te controleren om zo privéinformatie te herkennen en apart te plaatsen.

3.6 ARTIKEL 6. GERICHT ONDERZOEK

6.1 Bij zwaarwegende vermoedens van overtreding van deze, of andere, gedragscode door een medewerker heeft de UT het recht om een gericht onderzoek uit te voeren. Voor het uitvoeren van een gericht onderzoek is altijd een opdracht vanuit het CvB nodig. De UT garandeert dat een gericht onderzoek op een zorgvuldige manier wordt uitgevoerd.

3.7 ARTIKEL 7. CONSEQUENTIES VAN OVERTREDING

7.1 Bij handelen in strijd met deze gedragscode kan het College van Bestuur, afhankelijk van de aard en de ernst van de overtreding, onder meer de volgende sancties opleggen:
   a. tijdelijke of definitieve beperking in de toegang tot bepaalde ICT-faciliteiten;
   b. tijdelijk of definitief verbod tot het gebruik van bepaalde ICT-faciliteiten;
   c. betalen van kosten voortvloeiend uit het geconstateerde misbruik;
   d. overige sancties.

7.2 Sancties (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een geautomatiseerd uitgevoerde verwerking van persoonsgegevens, zoals een automatisch filter of blokkade. Voorts worden geen sancties getroffen zonder dat sprake is geweest van hoor en wederhoor.

7.3 In afwijking van het voorgaande is het mogelijk dat de Universiteit bij (geautomatiseerde) constatering van overlast of een beveiligingsrisico een (tijdelijke) blokkade van de betreffende faciliteit invoert.

3.8 ARTIKEL 8. SLOTBEPALING

8.1 Deze gedragscode wordt tweejaarlijks geëvalueerd.

8.2 In gevallen waarin deze gedragscode niet voorziet, beslist het College van Bestuur.

8.3 Deze gedragscode vervangt de Gedragscode ICT- en Internetgebruik Universiteit Twente 2009.

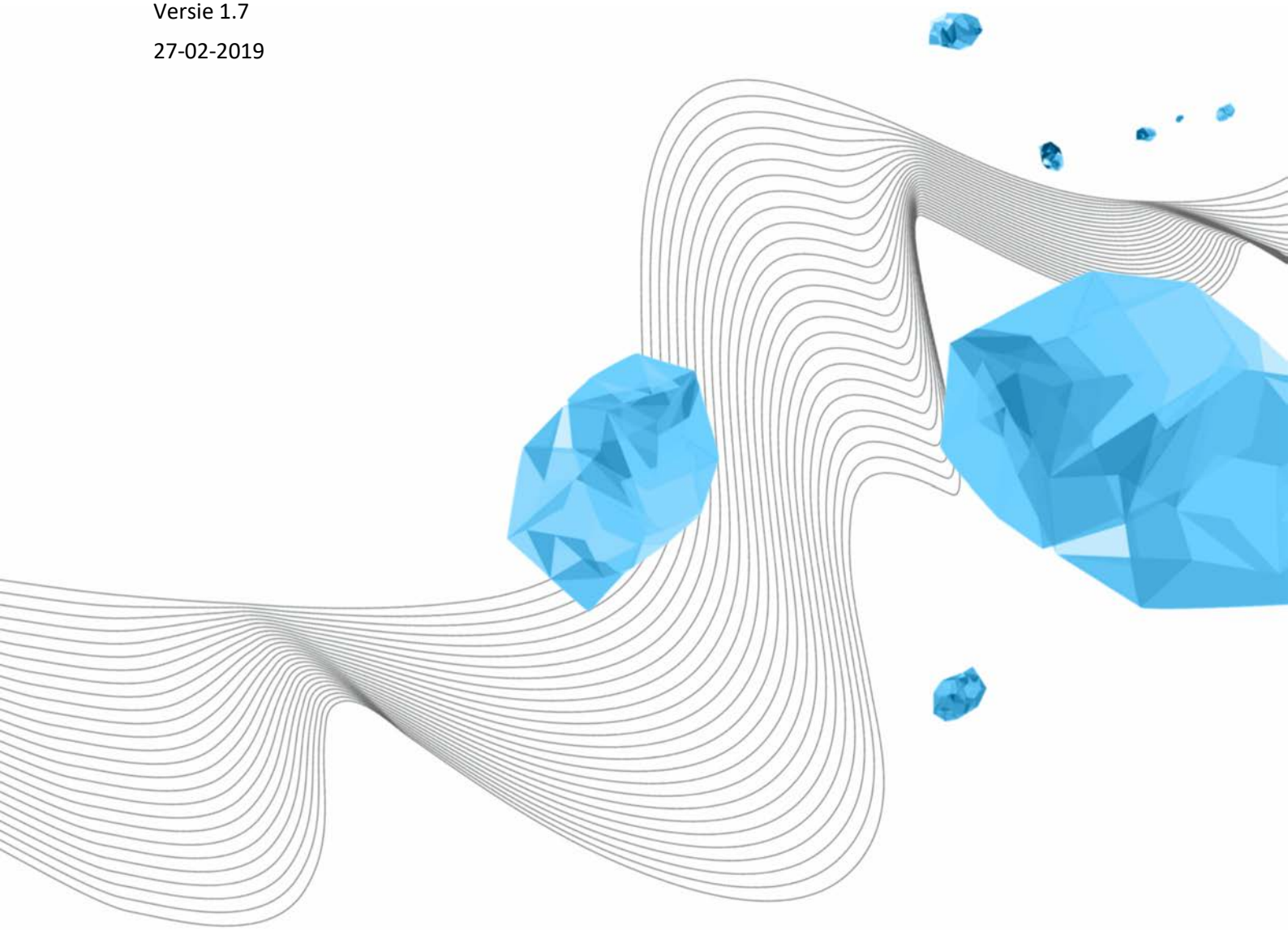
C O N C E P T

GEDRAGSCODE ICT-FUNCTIONARISSEN UNIVERSITEIT TWENTE

Brake - Loeve, A.A. te (LISA)

Versie 1.7

27-02-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Gedragscode ICT-functionarissen Universiteit Twente

KENMERK
UIM/181206/brk

VERSIE (STATUS)
1.7

DATUM
27-02-2019

AUTEUR(S)
Brake - Loeve, A.A. te (LISA)

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	13-12-2012	Wim Koolhoven	Definitieve versie
1.3	22-11-2018	Rianne te Brake	Herziene versie, leesbaarheid
1.4	06-12-2018	Rianne te Brake	Herziene versie, sjabloon aangepast
1.5	15-01-2019	Jan Evers	Opmerkingen MT LISA verwerkt
1.6	29-01-2019	Jan Evers	Opmerkingen MT LISA en Harma Evers verwerkt (o.a. WNRA-check)
1.7	26-02-2019	Jan Evers	Positief advies UCB

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.3	22-11-2018	Rianne te Brake	Jan Evers, Henk Swaters, Peter Peters, Marc Berenschot, Erna van der Zandt, Wim Olijslager
1.4	06-12-2018	Jan Evers	MT LISA
1.5	15-01-2019	Jan Evers	MT LISA en HR – Harma Evers
1.6	06-02-2019	Jan Evers	UCB
1.7	26-02-2019	Jan Evers	CvB

REFERENTIES

VERSIE	DATUM	AUTEUR(S)	TITEL

1 GEDRAGSCODE ICT-FUNCTIONARISSEN

Deze gedragscode is van toepassing op ICT-functionarissen van de Universiteit Twente, hierna genoemd de Universiteit. Hieronder vallen alle medewerkers die werken bij de dienst LISA, de functioneel beheerders van diverse applicaties en alle overige medewerkers die vanuit hun ICT-rol of -functie toegang hebben tot (vertrouwelijke) gegevens. Deze gedragscode is aanvullend op de Digitale gedragscode voor medewerkers Universiteit Twente (kenmerk UIM/181204/brk).

De ICT-functionaris is verplicht tot geheimhouding van alle (vertrouwelijke) gegevens waarvan hij (lees: hij of zij) tijdens zijn werkzaamheden kennisneemt en van gegevens waarbij uitdrukkelijk geheimhouding is opgelegd. Deze verplichting geldt ook na beëindiging van de werkzaamheden voor de Universiteit.

Deze verplichting tot geheimhouding geldt niet ten opzichte van andere ICT-functionarissen (collega's) wanneer het uitwisselen van gegevens noodzakelijk is voor de uitvoering van werkzaamheden door die collega.

Bij het uitvoeren van gericht onderzoek geldt de verplichting tot geheimhouding niet ten opzichte van de andere betrokkenen bij dit onderzoek, voor zover het uitwisselen noodzakelijk is voor het uitvoeren van het gericht onderzoek.

De ICT-functionaris is alleen bevoegd tot het lezen van documenten of e-mail of tot het meekijken met het gebruik door UT-medewerkers en -studenten van informatiesystemen (waaronder internet) met toestemming van die medewerker of student. Uitzondering hierop is wanneer er sprake is van gericht onderzoek naar een incident of naar niet-toegestaan gebruik van e-mail en/of informatiesysteem.

De ICT-functionaris voert gericht onderzoek uitsluitend uit na uitdrukkelijke opdracht door of namens het College van Bestuur, conform de hiervoor vastgesteld procedure.

De ICT-functionaris houdt zich bij zijn werk aan de bestaande wettelijke bepalingen en richtlijnen. Dit betreft onder meer de Algemene Verordening Gegevensbescherming, de Wet Computercriminaliteit en de Auteurswet en de uitwerkingen daarvan voor de Universiteit.

De ICT-functionaris zal bij zijn werk geen gedrag vertonen dat afbreuk doet aan het vertrouwen in de Universiteit of in het organisatieonderdeel van de Universiteit waarvoor hij werkt.

De ICT-functionaris zal bij het gebruik van informatie zo zorgvuldig mogelijk werken. Dit houdt in ieder geval in dat de ICT-functionaris maatregelen neemt om te voorkomen dat derden informatie te zien krijgen, die niet voor hen bestemd is.

De ICT-functionaris zal redelijkerwijs alles doen om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens op de voor hem toegankelijke informatiesystemen van de Universiteit te waarborgen.

De ICT-functionaris zal alle (mogelijke) incidenten met betrekking tot onjuist gebruik en/of misbruik van informatie(-systemen) direct melden bij het Computer Emergency Response Team (via cert@utwente.nl).

De ICT-functionaris heeft specifieke bevoegdheden, passend bij de werkzaamheden van zijn functie en/of taken. De ICT- functionaris mag deze bevoegdheden alleen gebruiken voor de werkzaamheden die voortvloeien uit zijn functie en/of taken. Daarnaast mag de ICT-functionaris deze bevoegdheden niet door anderen laten gebruiken.

Bij wijziging of beëindiging van werkzaamheden heeft de Universiteit de plicht de bevoegdheden van de ICT-functionaris dienovereenkomstig aan te passen. In voorkomende situaties kan van de ICT-functionaris gevraagd worden hieraan mee te werken.

Het niet naleven van deze Gedragscode kan leiden tot door of namens het College van Bestuur op te leggen sancties.

Deze gedragscode kan worden aangehaald als ‘Gedragscode ICT-functionarissen Universiteit Twente’.

Deze gedragscode wordt tweejaarlijks geëvalueerd.

Deze gedragscode vervangt de Gedragscode ICT-functionarissen Universiteit Twente gedateerd 13 december 2012.